



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Yusaku FUJII (Applicant)

ILLEGAL ACCESS DISCRIMINATING APPARATUS AND METHOD

Serial Number: 09/425,736

Filed: October 22, 1999

Appeal No.:

Group Art Unit: 2137

Examiner: Nadia Khoshnoodi

Submitted by:
Thomas E. Brown
Registration No. 44,450
Attorney for Appellants

WESTERMAN, HATTORI,
DANIELS & ADRIAN, LLP
1250 Connecticut Avenue NW, Suite 700
Washington, D.C. 20036
Tel (202) 822-1100
Fax (202) 822-1111

August 2, 2006



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re the Application of: **Yusaku FUJII et al.**

Group Art Unit: **2137**

Serial Number: **09/425,736**

Examiner: **Nadia Khoshnoodi**

Filed: **October 22, 1999**

Confirmation Number: **9951**

For: **ILLEGAL ACCESS DISCRIMINATING APPARATUS AND METHOD**

Attorney Docket Number: **991176**

Customer Number: **38834**

SUBMISSION OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

August 2, 2006

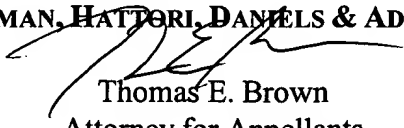
Sir:

Applicants submit herewith an Appeal Brief in the above-identified U.S. patent application.

Attached please find a check in the amount of \$620.00 (\$500.00 + \$120.00) to cover the cost for the Appeal Brief. If any additional fees are due in connection with this submission, please charge Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP


Thomas E. Brown
Attorney for Appellants
Registration No. 44,450
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

TEB/jl



**THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Appeal No: Unassigned

In re the Application of: **Yusaku FUJII et al.**

Group Art Unit: 2137

Serial No.: 09/425,736

Examiner: Nadia Khoshnoodi

Filed: October 22, 1999

Confirmation Number: 9951

For: ILLEGAL ACCESS DISCRIMINATING APPARATUS AND METHOD

Attorney Docket Number: 991176

Customer Number: 38834

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 2, 2006

Sir:

Applicants appeal the December 2, 2005 rejection of claims 1, 3-12 and 14-22.

Following the Notice of Appeal filed on May 2, 2006, the following is the Applicants' (now referred to hereinbelow as "appellants") Appeal Brief.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the subject application, which is:

Fujitsu Limited, 1-1, Kamikodanaka, 4-chome, Nakahara-ku, Kawasaki-shi, Japan by an

assignment recorded in the U.S. Patent and Trademark Office on **December 22, 1999**, at Reel

010453, Frame 0501.

00/03/2006 JADD01 00000025 09425736

01 FC:1402

500.00 OP

II. RELATED APPEALS AND INTERFERENCES

Appellants know of no other appeals or interference proceedings related to the present appeal.

III. STATUS OF CLAIMS

Claims 2 and 13 have been cancelled. Pending claims 1, 3-12 and 14-22 stand rejected. No claims are allowed or objected to. The claims on appeal are claims 1, 3-12 and 14-22.

IV. STATUS OF AMENDMENTS

An Amendment was filed under 37 CFR 1.111 on April 6, 2004 in which claims 1 and 12 were amended. An Amendment was filed under 37 CFR 1.116 on August 30, 2004 in which claims 1 and 12 were amended and claims 2 and 13 were cancelled. An Amendment was filed under 37 CFR 1.111 on September 6, 2005 in which claims 1 and 12 were amended. Each of these Amendments has been entered.

An Amendment was filed under 37 CFR 1.116 on April 3, 2006 in which claims 1, 11 and 22 were amended. In the Advisory Action dated April 26, 2006, it was indicated in item 7 that the Amendment filed on April 3, 2006 **would** be entered upon appeal. Accordingly, entry of the Amendment filed on April 3, 2006 is respectfully requested.

The list of claims in the Claim Appendix includes the claims as last amended in the Amendment filed on April 3, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to an illegal access discriminating apparatus and method.

With respect to claim 1, an illegal access discriminating apparatus (see *e.g.*, Fig. 1; and page 16, line 26 – page 17, line 1) that is placed in advanced of a user authentication system (see *e.g.*, page 18, lines 21-26) using biometrics which needs user information comprised of ID information (see *e.g.*, user input ID information 30 in Fig. 1; and page 17, lines 14-15) and organic information (see *e.g.*, organic information 32 in Fig. 1; and page 17, lines 14-15 and 20-25) comprising:

a first storing unit (see *e.g.*, organic information input storing unit 18 and ID information input storing unit 20 in Figs. 1 and 12B) for temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authenticated (see *e.g.*, page 19, lines 5-12),

a second storing unit (see *e.g.*, use information storing unit 22 in Figs. 1 and 2) for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time (see *e.g.*, page 9, line 13 – page 10, line 13; page 34, line 19 - page 35, line 4; page 36, lines 14-26; and page 40, lines 15-21), wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication (see *e.g.*, page 19, line 12 - page 20, line 3);

a comparing and collating unit (see *e.g.*, organic information collating unit 24 and ID information comparing unit 26 in Fig. 1) for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in

said second storing unit which were inputted (see *e.g.*, page 20, lines 4 – 25; page 49, line 21- page 50, line 3; and steps S1 and S2 of the flowchart in Fig. 17) and not previously registered in the past (*e.g.*, page 18, lines 4 – 26); and

a control unit (see *e.g.*, control unit 28 in Fig. 1) for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions (see *e.g.*, discriminating rule 3, page 21, line 21 – page 24, line 17; step S3 of the flowchart in Fig. 17; and page 50, lines 3-9) and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value (see *e.g.*, steps S4 and S5 of the flowchart in Fig. 17; and page 50, lines 6-16).

With respect to claim 12, an illegal access discriminating method (see *e.g.*, page 13, line 20 – page 14, line 13) that is placed in advanced of a user authentication system (see *e.g.*, page 18, lines 21-26) using biometric which needs user information comprised of ID information (see *e.g.*, user input ID information 30 in Fig. 1; and page 17, lines 14-15) and organic information (see *e.g.*, organic information 32 in Fig. 1; and page 17, lines 14-15 and 20-25), comprising:

a first storing step of temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authenticated (see *e.g.*, page 19, lines 5-12);

a second storing step of storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time (see *e.g.*, page 9, line 13 – page 10, line 13; page 34, line 19 - page 35, line 4; page 36, lines 15-26; and page 40, lines 15-21), wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication (see *e.g.*, page 19, line 12 - page 20, line 3);

a comparing and collating step of comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing step which were inputted in the past (see *e.g.*, page 20, lines 4 – 25; page 49, line 21-page 50, line 3; and steps S1 and S2 of the flowchart in Fig. 17); and

a control step of discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions (see *e.g.*, discriminating rule 3, page 21, line 21 – page 24, line 17; step S3 of the flowchart in Fig. 17; and page 50, lines 3-9) and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value (see *e.g.*, steps S4 and S5 of the flowchart in Fig. 17; and page 50, lines 6-16).

The illegal access discriminating apparatus of the present invention is different from an authentication apparatus in a service providing system.

The present invention does not provide a response to a request for a personal authentication by accessing a service providing system. In general, a service providing system has a configuration of giving an authentication for authorization to use to a user by registering user's ID and biometrics information in advance, and collating with these registered pieces of information. The present invention relates in contrast to an illegal access discriminating apparatus which detects an illegal access to a service providing apparatus. It detects an illegal access in a prior stage to the biometrics authentication (user ID+ biometrics) of a usual service providing system.

In the present invention, the comparing and collating unit compares the lasted inputted ID information and organic information with all the ID information and organic information that was stored in the second storing unit within a predetermined time. As such, for example, as discussed on page 23, lines 10-16 of the present specification, when the first pair of ID and organic information (ID1, LB1) is stored in the second storing unit at time t1, the first pair (ID1, LB1) can not be compared to other pairs for coincidence, since no other relevant pairs have been stored in the second storing unit. As further discussed on page 23, lines 15-25, when a second pair (ID2, LB1) is inputted at time t2, see Fig. 3, the second pair (ID2, LB1) can be compared against the first pair (ID1, LB1), since the first pair has been previously stored in the second storing unit. Moreover, since the ID information of the first and second pairs coincide; and the organic information of the first and second pair do not coincide, discriminating rule 1 (predetermined condition) is satisfied and the control unit 28 determines that an illegal access has been made.

In a preferred embodiment, for example, as discussed in page 26, lines 17 – page 27, line 5, the discriminating rule 3 (predetermined condition) is satisfied when the ID information does not coincide and the organic information coincides or when the ID information coincides and the organic information does not coincide on the basis on the comparison and collation results. Moreover, discriminating rule 3 can be modified to correspond to discriminating rule 6, see pages 48 and 49, which includes the same predetermined conditions as rule 3, but only determines that an illegal access has been made by an attacker when the number of

predetermined conditions that have been satisfied exceeds a predetermined value, see step S4 of Fig. 17.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

- A. The rejection of claims 11 and 22 under 35 USC 112, second paragraph, as failing 35 U.S.C. § 112, second paragraph, as being indefinite.
- B. The rejection of claims 1, 5 and 12 under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406) in view of McNair (USP 5,276,444).
- C. The rejection of claims 3, 4, 6-11, 12 and 14-22 under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406), and further in view of McNair (USP 5,276,444) and Gressel (USP 6,311,272).

VII. ARGUMENTS

- A. **Rejection of claims 11 and 22 under 35 USC 112, second paragraph, as failing 35 U.S.C. § 112, second paragraph, as being indefinite.**

Claims 11 and 22

It is respectfully submitted that claims 11 and 22 were each amended in the amendment dated April 3, 2006 in order to resolve the antecedent basis issue concerning the phrase, “a service providing system.” Accordingly, withdrawal of this rejection is respectfully requested.

- B. **Rejection of claims 1, 5 and 12 under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406) in view of McNair (USP 5,276,444).**

Claims 1 and 12

Independent claim 1 calls for *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication.* Independent claim 12 includes similar features.

In addition, claim 1 calls for *a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past.* Again, independent claim 12 includes similar features.

The Examiner rejects the present invention by citing Moussa, col. 3, lines 24-33 and col. 5, lines 56-64. However, Moussa's document has no relevance to the present invention. The cited portions of Moussa give expression such as "an authentication fingerprint F" and "the data block fingerprint D with the fingerprint F it has stored in the authentic database". However, the term "fingerprint" referred to in the present invention concerns a human fingerprint ("origin information" recited in claim 1 of the present invention). The fingerprint in the cited reference means a hash value¹ (*1) of a certain data, as described in col. 4, lines 50-54.

¹ In the encryption sector of industry, a hash value used in an electronic signature or the like is often called a "fingerprint". For example, when performing an "https" communication upon entering a password in Internet Explorer, a key mark appears in the right bottom of the screen. If this is clicked, you will understand that a

This fact is evident from Moussa's document, col. 6, lines 64-67. This portion of Moussa gives a description, "The login service 140 generates a new fingerprint F* in response to the new data block 132, in like manner as the data block fingerprint D is computed in the sub-step 224(b)." This expresses that a new "fingerprint" is prepared from a data block 132. This means that a new fingerprint (hash value) is created from data written in the data block 132. It is not correct to interpret this fingerprint as being a human fingerprint which is invariable all the life.

Moreover, in response, the Examiner asserts, on page 2 of the Advisory Action dated April 26, 2006, that "Moussa et al. discuss in many different areas of the reference that they are in fact referring to a human fingerprint as in the present invention," and directs appellants attention to col. 1, lines 14-20; col. 1, lines 39-46; col. 2, lines 5-8; and col. 3, lines 20-37 of the applied reference of Moussa.

However, it is submitted that the disclosure in col. 1 is directed to the discussion of related art in the background section and fails to concern the preferred embodiments of Moussa; the disclosure in col. 2 merely mentions biometric information and is silent with regard to using a human fingerprint for authenticating a user; and the disclosure in col. 3 concerns the fingerprint F, which is "derived in response to the set of random values by computation of a CRC or hashing function." See col. 3, lines 49-51.

hash value in an open certificate used cryptographic communication is displayed by an expression "fingerprint". Popularly used hash values include "MD5 fingerprint" and "SHA1 fingerprint".

As such, it is submitted that the Examiner's comments that "[a]ll of these column/line numbers show that the biometric fingerprint was the original source of information for the data block," has no merit, since as discussed above the fingerprint F in Moussa is derived in response to the set of random values by computation of a CRC or hashing function.

In addition, it is submitted that Moussa is also simply not concerned with storing pairs of ID information and organic information which were inputted by arbitrary users **within predetermined time** (see *e.g.*, page 9, line 13 – page 10, line 13; page 34, line 19 - page 35, line 4; page 36, lines 14-26; page 37, lines 9-15; and page 40, lines 15-21). That is, in the present invention, the comparing and collating unit compares and collating the latest inputted ID information and organic information with all of ID information and organic information stored in the second storing unit which were inputted **within a predetermined time**, i.e. 15, 60 minutes (see *e.g.*, page 37, lines 9-15; and page 45, lines 15-21).

In view of the above, it is submitted that Moussa's document cannot therefore be an example of a publicly known document of the present invention.

As such, it is submitted that Moussa fails to disclose or fairly suggest the features of claim 1 concerning *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication; a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information*

and organic information stored in said second storing unit which were inputted and not previously registered in the past.

Moreover, it is submitted that the secondary reference of McNair fails to teach or fairly suggest these above-noted drawbacks and deficiencies of the primary reference of Moussa.

Further, the Examiner correctly acknowledges (in the bridging sentence between pages 4 and 5 of the Action) that the primary reference of Moussa also fails to disclose the features of claim 1 concerning *a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.*

In order to compensate for these deficiencies of Moussa, the Examiner relies on the secondary reference of McNair and contends that McNair “teaches a threshold per biometric sample type that can possibly be used by each individual in order to indicate an attacker in the event of numerous unsuccessful authentication attempts,” (see, lines 1-3, page 5 of the Action).

However, it is respectfully submitted that while McNair may be concerned with a “try again” threshold, in which access is denied but the requester may be allowed to supply a different form of authentication information to obtain access, McNair is completely silent with regard to *discriminating authentication demand by an attacker by counting the number of said*

comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value, as called for in claim 1.

That is, it is respectfully submitted that the Examiner has failed to appreciate that McNair is simply not concerned with counting the number of comparing-collating results which **satisfy predetermined conditions** and judging authentication demand as the one by an attacker **if the counted number exceeds a predetermined value.**

Further, with regard to Gressel, the Examiner describes only the setting of such reference. Gressel says only that in an environment under supervision by a security camera or the like, it suffices to ensure a threshold value of a personal refusal rate of about once per 500, i.e., an FAR threshold of 100 is reasonable. This is followed by the cited portion (col. 10, Lines 35-39) which states only that a looser threshold of 200 will do in a placed of a higher frequency of use such as an amusement park, and contains no expression relating to the present invention.

As such, in view of the above, it is respectfully submitted that neither Moussa, McNair, nor Gressel, singly or in combination, disclose or fairly suggest the features of claim 1 concerning *a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication; a comparing and collating unit for comparing and collating the latest*

inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past; and a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.

- C. Rejection of claims 3, 4, 6-11, 12 and 14-22 under 35 U.S.C. § 103(a) as being unpatentable over Moussa et al. (USP 6,035,406), and further in view of McNair (USP 5,276,444) and Gressel (USP 6,311,272).**

Claims 3 and 14:

The Examiner contends that Moussa, when viewed with McNair and Gressel, discloses what is presently taught in claim 3. The Examiner states the Moussa and McNair do not disclose:

“a control unit [that] determines that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of said comparing and collating unit.”

The Examiner however, asserts that Gressel “teaches two typical proximity thresholds for biometric sampling, which are monitored for imposters attempting to enter unauthorized,” (col. 10, lines 26-34), and that “3% of the population would be rejected regardless of the value of the

threshold” and that “human intervention then becomes necessary to process the applicant,” (col. 10, lines 48-54).

Lines 26-34 of Gressel explain figure 9A, which is a graph describing the False Rejection Rate (FRR) and False Acceptance Rate (FAR) of a “Digi-2 finger geometry identification device.”² As would be predicted by one ordinarily skilled in the art, false rejections increase as the verification threshold criteria tightens, and false acceptances decrease. As expected, the opposite results are attained if the verification threshold criteria are loosened.

It is respectfully submitted that the passages in Gressel, cited by the Examiner, do not disclose what is taught in claims 3 (recited above), and 14, and have little if any relevance to the present invention.

Claims 4 and 15:

The Examiner contends that when Moussa is viewed in light of McNair and Gressel, it would have been obvious to one ordinarily skilled in the art to combine the three, and that therefore claims 4 and 15 were previously disclosed. Claim 4 involves:

said control unit determines that there is the authentication demand by the illegal access person in the case where the comparison result by said comparing and collating unity between the inputted ID information and the past ID information inputted from a same terminal position within a predetermined time indicates dissidence.

² As disclosed in Gressel, a “Digi-2 finger geometry identification device” is an electro-optical fingerprint reader, which is publicly available.

In other words, the present invention is able to factor in; the difference in time between two possible illegal access attempts, and whether or not the same terminal was used, in order to help determine if an illegal access was being attempted.

Gressel discloses that “upon successful completion of the bio-test, the user’s biometric features are encoded into the smart card,” (column 12, lines 42-43). The Examiner contends that “it would have been obvious to combine Gressel’s teachings to Moussa and McNair, because it would allow only a reasonable amount of time to transfer the biometric features, thus discouraging break-ins.”

The Examiner is arguing that the amount of time between inputting two different identification methods (such as performing a bio-test and encoding a smartcard), during the same overall access attempt, is the same as the amount of time between two different and distinct access attempts. Claims 4 and 15 each call for discerning an illegal access attempt using the latter method, while it is asserted by the Examiner that Gressel implies the former method. As is apparent on its face, the two methods are not the same.

For at least these reasons, Moussa, McNair, and Gressel, when viewed singly or in any combination, do not disclose or fairly suggest the elements of claims 4 or 15.

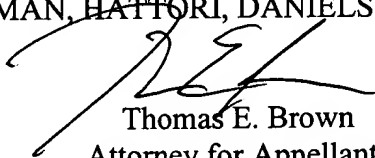
VIII. CONCLUSION

For the above reasons, Appellants request that the Board of Patent Appeals and Interferences reverse the Examiner's rejections of claims 1, 3-12 and 14-22.

In the event this paper is not timely filed, appellants hereby petition for an appropriate extension of time. The fee for any such extension may be charged to our Deposit Account No. 50-2866, along with any other additional fees which may be required with respect to this paper.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



Thomas E. Brown
Attorney for Appellants
Reg. No. 44,450

TEB/jl

Enclosures: Claims appendix
Evidence appendix
Related proceedings appendix

CLAIMS APPENDIX

Claim 1 (Previously Presented): An illegal access discriminating apparatus that is placed in advanced of a user authentication system using biometrics which needs user information comprised of ID information and organic information comprising:

a first storing unit for temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authenticated,

a second storing unit for storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication;

a comparing and collating unit for comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing unit which were inputted and not previously registered in the past; and

a control unit for discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.

Claim 2 (Cancelled).

Claim 3 (Original): An apparatus according to claim 1, wherein said control unit determines that there is the authentication demand by the illegal access person in the case where

the ID information does not coincide and the organic information coincides or the case where the ID information coincides and the organic information does not coincide on the basis of the output of said comparing and collating unit.

Claim 4 (Original): An apparatus according to claim 1, wherein said storing unit stores a telephone number serving as a transmitting source, a terminal position such as a network address, and an input time in correspondence to the ID information and organic information which were inputted in the past, and

said control unit determines that there is the authentication demand by the illegal access person in the case where the comparison result by said comparing and collating unit between the inputted ID information and the past ID information inputted from a same terminal position within a predetermined time indicates dissidence.

Claim 5 (Original): An apparatus according to claim 1, wherein said control unit discriminates whether the past ID information has a serial number for the inputted ID information or not and, when it is determined that the past ID information has the serial number, said control unit determines that there is the authentication demand by the illegal access person at a predetermined designated number of times.

Claim 6 (Original): An apparatus according to claim 1, wherein when the inputted organic information and the organic information which was inputted in the past coincide, said control unit detects a combination in which the organic information coincides and the ID

information differs, and when the number of said combinations reaches a predetermined number, said control unit determines that there is the authentication demand by the illegal access person.

Claim 7 (Original): An apparatus according to claim 1, wherein said comparing and collating unit comprises:

an ID information comparing unit for comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence; and

an organic information collating unit for comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained, and generating a signal indicative of dissidence of the organic information in the case where a value less than said predetermined coincidence degree is obtained.

Claim 8 (Original): An apparatus according to claim 1, further comprising a timer unit for measuring a time, and wherein the ID information and organic information which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured by said timer unit are erased and excluded from targets of the comparison and collation.

Claim 9 (Original): An apparatus according to claim 1, wherein
said storing unit stores a telephone number serving as a transmitting source and a
terminal position such as a network address or the like together with the ID information and
organic information which were inputted in the past, and
said comparing and collating unit compares and collates the inputted ID information and
organic information with the ID information and organic information which were inputted in the
past from a same terminal position.

Claim 10 (Original): An apparatus according to claim 1, further comprising:
an authentication demand terminal address recording unit for recording the number of
times of authentication demand every terminal address; and
a same terminal access detecting unit for detecting that the authentication demand of a
predetermined number or more has been performed within a predetermined time with reference
to said authentication demand terminal address, activating said comparing and collating unit and
said control unit, and allowing an illegal access to be discriminated.

Claim 11 (Previously Presented): An apparatus according to claim 1, wherein when it is
determined that there is the authentication demand by the illegal access person, said control unit
automatically notifies an administrator of a service providing system of a result of said
discrimination.

Claim 12 (Previously Presented): An illegal access discriminating method that is placed in advanced of a user authentication system using biometric which needs user information comprised of ID information and organic information, comprising:

a first storing step of temporarily storing the latest pair of ID information and organic information inputted by a user when the user is being authenticated;

a second storing step of storing pairs of ID information and organic information which were inputted by arbitrary users within predetermined time, wherein said ID information and organic information is transferred from said first storing unit to said second storing unit after each authentication;

a comparing and collating step of comparing and collating the latest inputted ID information and organic information with all of ID information and organic information stored in said second storing step which were inputted in the past; and

a control step of discriminating authentication demand by an attacker by counting the number of said comparing-collating results which satisfy predetermined conditions and judging authentication demand as the one by an attacker if said counted number exceeds predetermined value.

Claim 13 (Cancelled).

Claim 14 (Original): A method according to claim 12, wherein in said control step, it is determined that there is the authentication demand by the illegal access person in the case where the ID information does not coincide and the organic information coincides or the case where the

ID information coincides and the organic information does not coincide on the basis of the output in said comparing and collating step.

Claim 15 (Original): A method according to claim 12, wherein
in said storing step, a telephone number serving as a transmitting source, a terminal position such as a network address, and an input time in correspondence to the ID information and organic information which were inputted in the past are stored, and
in said control step, it is determined that there is the authentication demand by the illegal access person in the case where the comparison result in said comparing and collating step between the inputted ID information and the past ID information inputted from a same terminal position within a predetermined time indicates dissidence.

Claim 16 (Original): A method according to claim 12, wherein in said control step, whether the past ID information has a serial number for the inputted ID information or not is discriminated and, when it is determined that the past ID information has the serial number, it is determined that there is the authentication demand by the illegal access person at a predetermined designated number of times.

Claim 17 (Original): A method according to claim 12, wherein in said control step, when the inputted organic information and the organic information which was inputted in the past coincide, a combination in which the organic information coincides and the ID information

differs is detected, and when the number of said combinations reaches a predetermined number, it is determined that there is the authentication demand by the illegal access person.

Claim 18 (Original): A method according to claim 12, wherein said comparing and collating step comprises:

an ID information comparing step of comparing the inputted ID information and the ID information which was inputted in the past and generating a signal indicative of coincidence or dissidence; and

an organic information collating step of comparing the inputted organic information and the organic information which was inputted in the past, generating a signal indicative of coincidence of the organic information in the case where a value of a predetermined coincidence degree or more is obtained, and generating a signal indicative of dissidence of the organic information in the case where a value less than said predetermined coincidence degree is obtained.

Claim 19 (Original): A method according to claim 12, further comprising a timer step of measuring a time, and wherein the ID information and organic information which were inputted in the past after the elapse of a predetermined time from the storage on the basis of time information measured in said timer step are erased and excluded from targets of the comparison and collation.

Claim 20 (Original): A method according to claim 12, wherein

in said storing step, a telephone number serving as a transmitting source and a terminal position such as a network address or the like are stored together with the ID information and organic information which were inputted in the past, and

in said comparing and collating step, the inputted ID information and organic information with the ID information and organic information which were inputted in the past from a same terminal position are compared and collated.

Claim 21 (Original): A method according to claim 12, further comprising:

an authentication demand terminal address recording step of recording the number of times of authentication demand every terminal address; and

a same terminal access detecting step of detecting that the authentication demand of a predetermined number or more has been performed within a predetermined time with reference to said authentication demand terminal address, activating said comparing and collating step and said control step, and allowing an illegal access to be discriminated.

Claim 22 (Previously Presented): A method according to claim 12, wherein in said control step, when it is determined that there is the authentication demand by the illegal access person, a result of said discrimination is automatically notified to an administrator of a service providing system.

EVIDENCE APPENDIX

No evidence under 37 C.F.R. § 41.37(c)(1)(ix) is submitted.

RELATED PROCEEDING APPENDIX

No decisions under 37 C.F.R. § 41.37(c)(1)(x) are rendered.